Symantec AntiVirus™ Corporate Edition Справочник



Symantec AntiVirus™ Corporate Edition Справочник

Программное обеспечение, описанное в этой книге, поставляется с лицензионным соглашением и может использоваться только при соблюдении условий этого соглашения.

Версия документации: 8.0

Авторские права

Товарные знаки

Напечатано в Ирландии.

10 9 8 7 6 5 4 3 2 1

Оглавление

Глава 4 Средство Importer

Глава 5 Службы Windows XP/2000/NT

Глава 6 Записи журнала событий Windows XP/2000/NT

Алфавитный указатель

Обслуживание и техническая поддержка

Об этом справочнике

Разделы справочника

Этот справочник содержит техническую информацию о продукте Symantec AntiVirus Corporate Edition и программах, записанных на компакт-диске Symantec AntiVirus Corporate Edition. Он предназначен для системных администраторов и других лиц, ответственных за установку и обслуживание продукта в сетевой корпоративной среде.

В Табл. 1-1 перечислены разделы этого справочника.

Табл. 1-1 Разделы справочника

Раздел	Описание
Сценарии	В этой главе приведены примеры работы с Symantec AntiVirus Corporate Edition в трех организациях различного размера: средней, большой и очень большой. Хотя ни один из этих примеров может не соответствовать в точности вашей компании, с ними рекомендуется ознакомиться, чтобы представлять себе, как система безопасности реализована в других компаниях, и какие соображения были приняты во внимание при построении этой системы.
Средство Reset ACL	Многие настройки конфигурации Symantec AntiVirus Corporate Edition хранятся в реестре Windows. Средство Reset ACL позволяет ограничить доступ к соответствующим разделам реестра операционной системы Windows XP/2000/NT для обычных пользователей.

Табл. 1-1 Разделы справочника

Раздел	Описание
Средство Importer	Средство Importer - это утилита командной строки, предназначенная для работы с Symantec System Center. С ее помощью можно импортировать в кэш адресов необходимое количество наборов, состоящих из имен компьютеров и IP-адресов. Это позволит Symantec AntiVirus Corporate Edition обнаруживать компьютеры в сети даже в том случае, если службы WINS/DNS не поддерживаются.
Службы Windows XP/2000/NT	В этой главе перечислены названия служб, автоматически запускаемых программой Symantec AntiVirus Corporate Edition и Symantec System Center. Имена представлены в том формате, в котором они показаны в панели управления службами Windows XP/2000/NT.
Записи журнала событий Windows XP/2000/NT	В этой главе перечислены и описаны связанные с Symantec AntiVirus Corporate Edition события, информация о которых заносится в журнал событий Windows.

Глава 2

Пользовательские сценарии

Эта глава содержит следующие разделы:

- Сценарий 1: Организация среднего размера
- Сценарий 2: Большая организация
- Сценарий 3: Очень большая организация

Сценарий 1: Организация среднего размера

Допустим, что в организации есть один основной офис и несколько удаленных пользователей. Рабочую среду этой организации можно описать следующим образом:

- В организации установлено более 1000 рабочих станций, на 96% которых применяется Windows 98/Me. В службе MIS на настольных компьютерах установлена операционная система Windows 2000/XP.
- Несколько пользователей работают не выходя из дома; на их компьютерах установлена операционная система Windows 98/Me.
- На 98% серверов применяется NetWare. В организации также есть несколько серверов Windows 2000.
- В организации широко используются программы Microsoft Word и Microsoft Excel.

Установка Symantec AntiVirus Corporate Edition в организации среднего размера

Symantec AntiVirus Corporate Edition следует устанавливать следующим образом:

- С помощью Symantec Packager необходимо создать пакеты для последующего развертывания. Для развертывания применяются несколько специальных средств. Некоторые администраторы создают сценарии регистрации для установки без вывода сообщений, другие же пользуются средствами Web-установки клиентов.
- Удаленным пользователям предоставляются компакт-диски для установки автономных клиентов Symantec AntiVirus Corporate Edition.

Обработка оповещений в организации среднего размера

Оповещения обрабатываются в организациях среднего размера следующим образом:

- На первичном сервере устанавливается AMS^2. В случае обнаружения вируса на адрес администратора отправляется электронное письмо.
- Журналы AMS^2 отслеживаются с помощью программы Symantec System Center для выявления событий или вирусов, требующих особого внимания.

Защита от вирусов в организации среднего размера

Организации среднего размера строят систему защиты от вирусов следующим образом:

- На серверах NetWare устанавливается программа-сервер Symantec AntiVirus Corporate Edition.
- Рабочие станции защищаются с помощью клиента Symantec AntiVirus Corporate Edition. Параметры Symantec AntiVirus Corporate Edition, применяемые на рабочих станциях, определяются MIS. Служба MIS блокирует доступ к параметрам Symantec AntiVirus Corporate Edition, чтобы избежать несанкционированного изменения способа защиты от вирусов пользователями.
- На одну из рабочих станций Windows 2000 Professional администратор устанавливает программу Symantec System Center для администрирования антивирусных функций.
- Один из вспомогательных серверов Windows 2000 выбирается в качестве первичного. Применение вспомогательного сервера позволит не занимать ресурсы сервера, необходимые для повседневной работы. Первичный сервер обновляется с помощью функции LiveUpdate автоматически. Затем описания вирусов распространяются на все серверы NetWare методом передачи вирусных описаний (Virus Definition Transport Method).
- Служба MIS объединяет в одну группу все рабочие станции, которые она сочтет наименее защищенными. Параметры Symantec AntiVirus Corporate Edition для этой группы настраиваются таким образом, чтобы обеспечить для входящих в нее рабочих станций наибольший уровень защиты.
- Оповещения об обнаружении вирусов и обновления описаний постоянно отслеживаются с помощью консоли Symantec System Center. Администратор регулярно проверяет журнал событий и журнал вирусов для выявления событий или вирусов, требующих повышенного внимания.

- Большинство серверов NetWare являются серверами приложений и файловыми серверами. Пользователи часто обращаются к файлам на этих серверах. По умолчанию система постоянной защиты сервера Symantec AntiVirus Corporate Edition осматривает файлы при их создании, переименовании, перемещении, открытии, копировании, запуске и сохранении. Служба MIS настраивает постоянную защиту сервера таким образом, чтобы файлы осматривались только при их создании, переименовании или перемещении. Это позволит повысить производительность за счет сокращения числа отслеживаемых операций.
- Администратор планирует осмотр серверной группы для проверки всех серверов Symantec AntiVirus Corporate Edition в нерабочее время. Осмотр должен быть запланирован на время, не совпадающее с временем выполняющегося каждую ночь резервного копирования, чтобы эти задачи не пересекались друг с другом.
- Администратор также составляет план еженедельного осмотра клиентов.

Обновление описаний вирусов в организации среднего размера

Организации среднего размера обновляют описания вирусов следующим образом:

- Серверы NetWare не могут использовать метод автоматического обновления вирусных описаний, поскольку их нельзя настроить для подключения по протоколу FTP. Поэтому администратор создает пакетный файл, запускаемый по расписанию дважды в неделю. С его помощью файл описаний загружается с FTP-сайта компании Symantec и копируется в каталог NAV первичного сервера.
- Вторичные серверы автоматически получают обновления с первичного сервера.
- Большинство клиентов Symantec AntiVirus Corporate Edition автоматически получают описания вирусов с родительского сервера, используя метод передачи вирусных описаний. Как только родительский сервер получает новые описания, он незамедлительно начинает отправку обновлений клиентам. Родительский сервер может обновлять несколько клиентов одновременно, по одному клиенту в каждой подсети, чтобы сократить сетевой трафик.
- Удаленные клиенты получают обновленные описания от Symantec с помощью функции LiveUpdate.

Сценарий 2: Большая организация

Пусть организация имеет один центральный офис и 50 филиалов, расположенных в различных районах Новой Англии. Рабочую среду этой организации можно описать следующим образом:

- В пяти зданиях центрального офиса установлено 5000 рабочих станций. В каждом филиале используется около 100 рабочих станций.
- В организации 420 серверов, на 95% которых установлена операционная система Windows NT/2000, а на 5% – NetWare. Большинство серверов расположены в центральном офисе, а многие филиалы обходятся без локального сервера. В организации применяются два терминальных сервера.
- В организации имеется 10 000 рабочих станций, 50% которых работают под управлением Windows 2000, а 50% – под управлением Windows 98/Me/XP.
- К терминальным серверам подключено 60 простых клиентов.
- Филиалы подключены к центральному офису через глобальную сеть по каналу с пропускной способностью 56K, а центральный офис имеет выход в Интернет по каналу 128K. В связи с ограниченной пропускной способностью, сетевой трафик по этим каналам рекомендуется свести к минимуму.
- В организации широко используются программы Microsoft Exchange, Microsoft Word и Microsoft Windows. Большая часть рабочих станций в этой организации подвержена высокому риску заражения макровирусами, распространения вирусов по электронной почте и комплексным атакам.

Установка системы защиты клиентов в большой организации

Система защиты устанавливается на клиентах в большой организации следующим образом:

- В главном офисе MIS передает на локальные компьютеры пакеты установки и миграции с помощью Novell ZENworks. С помощью Symantec Packager необходимо создать выборочные пакеты для последующего развертывания. Для экономии места на жестких дисках пользователей рекомендуется устанавливать только те компоненты Symantec AntiVirus Corporate Edition, которые требуются на данном компьютере. MIS создает пакеты для установки без выдачи сообщений. Кроме того, администраторы указывают, какие настройки

продукта Symantec AntiVirus Corporate Edition пользователи могут изменять самостоятельно.

- Филиалы не используют Symantec Packager для развертывания пакетов из-за ограниченной пропускной способности сети. Пользователи в филиалах применяют для установки Symantec AntiVirus Corporate Edition web-интерфейс. Администраторы отправляют таким пользователям электронные сообщения, содержащие необходимые инструкции и ссылку (URL) на программу Web-установки.

Обработка оповещений в большой организации

Оповещения обрабатываются в больших организациях следующим образом:

- Первичные серверы являются также серверами AMS^2. Им передаются оповещения со всех остальных серверов (включая консоль терминального сервера) и рабочих станций.
- При обнаружении вируса система AMS^2 отправляет электронное письмо администратору, ответственному за защиту от вирусов.
- Журналы AMS^2 отслеживаются с помощью программы Symantec System Center для выявления событий, вирусов или комплексных атак, требующих особого внимания.

Защита от вирусов в большой организации

Большие организации строят систему защиты от вирусов следующим образом:

- Для защиты компьютеров организации от вирусов из сети Интернет применяется Symantec Enterprise Firewall.
- Сервер Microsoft Exchange защищается программой Symantec AntiVirus/Filtering for Microsoft Exchange.
- Все серверы NetWare защищаются с помощью сервера Symantec AntiVirus Corporate Edition.
- Все серверы Windows NT/2000, управляющие клиентами Symantec AntiVirus Corporate Edition, защищаются с помощью сервера Symantec AntiVirus Corporate Edition. Безопасность остальных серверов Windows NT/2000 обеспечивается с помощью клиентов Symantec AntiVirus Corporate Edition.
- На терминальных серверах запускается сервер Symantec AntiVirus Corporate Edition.

- Рабочие станции защищаются с помощью Symantec AntiVirus Corporate Edition. Параметры Symantec AntiVirus Corporate Edition, применяемые на рабочих станциях, определяются MIS. Электронную почту просматривает специальный модуль Symantec AntiVirus Corporate Edition. MIS блокирует доступ пользователей к параметрам настройки Symantec AntiVirus Corporate Edition, чтобы избежать несанкционированного изменения параметров системы защиты от вирусов.
- Служба MIS создает несколько групп серверов и клиентов Symantec AntiVirus Corporate Edition. Перед созданием этих групп разрабатывается подробный план. План должен учитывать многочисленные аспекты, связанные с физической конфигурацией сервера, быстродействием линии связи и уровнем безопасности, необходимым для отделов и групп пользователей с различной степенью уязвимости.
- Программа Symantec System Center установлена в центральном офисе, поэтому администраторы могут настраивать параметры антивирусной защиты централизованно.
- Серверы, на которых работает сервер Symantec AntiVirus Corporate Edition, разбиты на несколько групп. В одну группу попадают, например, терминальные серверы и серверы NetWare с Symantec AntiVirus Corporate Edition, поскольку их требования к безопасности, загрузке и функциям похожи.
- Число клиентов, подключенных к одному родительскому серверу, лежит в диапазоне от 3500 до 15000. Каждую минуту с родительским сервером общаются примерно десять клиентов.
- Для различных отделов организации созданы различные группы клиентов. Например, компьютеры разработчиков объединены в группу клиентов с наименьшими требованиями к безопасности. Компьютеры в отделе работы с клиентами наиболее подвержены атакам почтовых вирусов. На компьютерах из этой группы блокированы все настройки клиента Symantec AntiVirus Corporate Edition.
- Локальные и удаленные клиенты разбиты на разные группы клиентов, поскольку они используют разные методы обновления вирусных описаний.
- На серверах Windows NT/2000, не являющихся родительскими, работает клиент Symantec AntiVirus Corporate Edition. Пользователи часто обращаются к файлам на этих серверах. По умолчанию система постоянной защиты клиента Symantec AntiVirus Corporate Edition

осматривает файлы при их создании, переименовании, перемещении, открытии, копировании, запуске и сохранении. Служба MIS настраивает постоянную защиту клиента таким образом, чтобы файлы осматривались только при их создании, переименовании или перемещении. Это позволит повысить производительность за счет сокращения числа отслеживаемых операций.

- Клиенты настраиваются таким образом, что если пользователь отключит постоянную защиту файловой системы, она будет автоматически включена через тридцать минут.
- Программа Symantec AntiVirus Corporate Edition пересылает зараженные файлы, которые не удалось исправить, на сервер Центрального изолятора. Администратор передает подозрительные файлы в группу Symantec Security Response для анализа. Symantec Security Response анализирует представленные файлы и возвращает администратору новые вирусные описания или другие средства для устранения вирусов.
- Администратор планирует осмотр серверной группы для проверки всех серверов Symantec AntiVirus Corporate Edition в нерабочее время. Осмотр должен быть запланирован на время, не совпадающее с временем выполняющегося каждую ночь резервного копирования, чтобы эти задачи не пересекались друг с другом.
- Администраторы настраивают клиенты таким образом, чтобы осмотр выполнялся через каждые 5 дней. В окне Параметры клиента (только для администратора) Symantec AntiVirus Corporate Edition был выбран параметр приостановки планового осмотра, если клиент работает от батарей. Поэтому, если переносной компьютер питается от батарей, то плановый осмотр будет отложен до того момента, когда будет восстановлено обычное питание.
- На компьютерах с операционной системой Windows настраиваются ресурсы процессора, занимаемые при ручном или плановом осмотре. Это позволяет загружать процессор в промежутки времени, когда он простаивает, минимизируя тем самым влияние на обычную работу пользователя.

Обновление описаний вирусов в большой организации

Большие организации обновляют описания вирусов следующим образом:

- Подход, применяемый MIS, призван сократить объем передаваемых по сети данных. Администратор настроил сервер FTP таким образом, чтобы часть внутренней сети компании выполняла роль сервера

LiveUpdate. Это не специально выделенный сервер LiveUpdate или Symantec AntiVirus Corporate Edition. Программа администрирования LiveUpdate загружает обновления продуктов Symantec AntiVirus Corporate Edition и файлы вирусных описаний с сервера FTP компании Symantec на сервер FTP в центральном офисе.

- Программа администрирования LiveUpdate настроена на загрузку новых пакетов ежедневно, в нерабочее время.
- Первичный сервер получает обновления описаний вирусов с внутреннего сервера LiveUpdate. Затем он передает полученные обновления на вторичные серверы.
- Родительские серверы распространяют обновления методом передачи вирусных описаний. Размер файла с описаниями вирусов не велик. Служба MIS настроила в Symantec AntiVirus Corporate Edition наиболее эффективный способ передачи описаний вирусов. Описания передаются несколькими потоками, от самых быстрых к самым медленным. Каждый поток разворачивается в одной подсети до тех пор, пока не будут обслужены все клиенты этой подсети.

Сценарий 3: Очень большая организация

Эта организация имеет офисы, расположенные по всему миру. Организация имеет 150 офисов в США, в каждом из которых работает от 20 до 3000 сотрудников. Рабочую среду этой организации можно описать следующим образом:

- 2500 серверов, из которых 10% используют NetWare, 20% - Windows NT, 65% – Windows 2000, а 5% – Unix.
- Всего в организации 35000 рабочих станций, расположенных в США, из которых 50% используют Windows 98/Me/XP, а 50% – Windows NT/2000.
- Многие пользователи Windows NT/2000 не имеют прав администратора на своих рабочих станциях.
- Многие компьютеры с операционной системой Windows являются портативными компьютерами.
- Администраторы пользуются специальной служебной программой для установки программного обеспечения на все рабочие станции.
- Широко используются программы Lotus Notes, Microsoft Exchange, Microsoft Word и Microsoft Windows.

В организации используется Tivoli SecureWay Risk Manager 3.7, поставляемый вместе с адаптером для Symantec AntiVirus Corporate Edition. С помощью этого адаптера Tivoli SecureWay Risk Manager может читать журналы событий Symantec AntiVirus Corporate Edition. Tivoli SecureWay Risk Manager собирает и показывает следующую информацию:

- Состояние обновления описаний вирусов.
- Хронологическую информацию о сканировании
- Статистику об общем числе заражений в организации

Установка Symantec AntiVirus Corporate Edition в очень большой организации

Symantec AntiVirus Corporate Edition следует устанавливать следующим образом:

- MIS распространяет пакеты для установки и миграции на локальные компьютеры с помощью Microsoft SMS. С помощью Symantec Packager необходимо создать пакеты для последующего развертывания. Различные пакеты распространяются с различных родительских серверов для каждой группы клиентов, в зависимости от расположения и специальных требований этих клиентов. Для экономии места на жестких дисках пользователей рекомендуется устанавливать только те компоненты Symantec AntiVirus Corporate Edition, которые требуются на данном компьютере. MIS создает пакеты для интерактивной установки. Кроме того, администраторы указывают, какие настройки продукта Symantec AntiVirus Corporate Edition пользователи могут изменять самостоятельно.
- Для пользователей портативных компьютеров разрабатывается специальный установочный компакт-диск Symantec AntiVirus Corporate Edition с аналогичным установочным пакетом.
- Небольшие филиалы, в которых не используется программа SMS, пользуются методом Web-установки для распространения установочных пакетов. Администраторы отправляют таким пользователям электронные сообщения, содержащие необходимые инструкции и ссылку (URL) на программу Web-установки.

Обработка оповещений, журналов и отчетов в очень большой организации

Оповещения, журналы и отчеты обрабатываются в очень больших организациях следующим образом:

- Информация о событиях Symantec AntiVirus Corporate Edition передается в Symantec Enterprise Security с помощью программы Collector Symantec AntiVirus Corporate Edition. С помощью Symantec Enterprise Security служба поддержки заносит в журнал сообщения, генерирует уведомления об оповещениях в качестве ответов на события, а также создает предопределенные и настраиваемые отчеты о состоянии событий.
- Для управления оповещениями и уведомлениями применяются пороговые значения. Для передачи уведомлений используются пейджеры, электронная почта и извещения SNMP.
- MIS запрашивает, фильтрует и сортирует информацию о событиях, чтобы определить, защита каких систем не была реализована, устарела или испытывает повышенное давление со стороны злоумышленников.
- На основании собранной информации служба MIS создает отчеты о событиях в текстовом и графическом виде. Некоторые отчеты предназначены для внутреннего пользования службой поддержки, другие же создаются для директоров и высшего руководства компании.

Защита от вирусов в очень большой организации

Очень большие организации строят систему защиты от вирусов следующим образом:

- Для защиты своего узла от заражения из сети Интернет, администраторы используют Symantec AntiVirus for SMTP Gateways.
- Серверы Lotus Notes защищаются программой Symantec AntiVirus/ Filtering for Domino.
- Серверы Microsoft Exchange защищаются программой Symantec AntiVirus/Filtering for Microsoft Exchange.
- Все серверы NetWare защищаются с помощью сервера Symantec AntiVirus Corporate Edition.
- Безопасность большей части серверов Windows NT/2000 обеспечивается с помощью клиентов Symantec AntiVirus Corporate Edition. Несколько выделенных серверов, которые являются частью

антивирусной системы организации, защищаются с помощью сервера Symantec AntiVirus Corporate Edition. Серверы NetWare и терминальные серверы также защищаются с помощью серверов Symantec AntiVirus Corporate Edition.

- Рабочие станции защищаются с помощью Symantec AntiVirus Corporate Edition. Параметры программы Symantec AntiVirus Corporate Edition, в том числе параметры защиты почтовых клиентов, указываются администраторами. Служба MIS блокирует доступ к параметрам Symantec AntiVirus Corporate Edition, чтобы избежать несанкционированного изменения способа защиты от вирусов пользователями. Для групп клиентов с особыми требованиями к безопасности создаются специальные конфигурации защиты от вирусов.
- Филиалы с высокоскоростными каналами связи объединяются в одну группу серверов с несколькими группами клиентов для разных отделов.
- Для некоторых филиалов с медленными линиями связи создаются отдельные группы серверов. Администратор каждого узла отвечает за его антивирусную защиту. Для некоторых филиалов с медленными линиями связи вместо групп серверов создаются родительские серверы. Они используют метод передачи вирусных описаний. Первичный сервер, расположенный в отделе автоматизации, передает файлы описания вирусов по каналу связи с пропускной способностью 56K. Родительские серверы передают клиентам файлы описания вирусов по локальной сети филиала. Если в небольшом филиале нет своего сервера, то описания передаются с удаленного родительского сервера. LiveUpdate запускается на клиентах в случайном порядке. Клиент проверяет, не был ли сеанс LiveUpdate запланирован на то время, когда компьютер был недоступен. Если это так, то LiveUpdate запускается сразу после включения компьютера.
- Почти всеми экземплярами Symantec AntiVirus Corporate Edition управляет служба поддержки организации (MIS). MIS поддерживает единую согласованную политику защиты клиентов от вирусов.
- В больших филиалах с медленными линиями связи есть свои администраторы. Консоль Symantec System Center запускается только в службе поддержки (MIS) и в таких филиалах. Администраторы в каждом филиале имеют пароли для доступа к группам серверов, за которые они отвечают.
- Для обеспечения должного уровня защиты создаются группы клиентов. Отдел продаж расположен в четырех различных офисах. Все

компьютеры этого отдела входят в группу клиентов отдела продаж. Отдел разработки расположен в одном офисе, однако также имеет собственную группу клиентов. Для компьютеров этой группы установлены менее жесткие параметры защиты, и разработчики могут отключать защиту на время компиляции программ.

- На серверах Windows NT/2000, не являющихся родительскими, работает клиент Symantec AntiVirus Corporate Edition. Пользователи часто обращаются к файлам на этих серверах. По умолчанию система постоянной защиты клиента Symantec AntiVirus Corporate Edition осматривает файлы при их создании, переименовании, перемещении, открытии, копировании, запуске и сохранении. Служба MIS настраивает постоянную защиту клиента таким образом, чтобы файлы осматривались только при их создании, переименовании или перемещении. Это позволит повысить производительность за счет сокращения числа отслеживаемых операций.
- Для пользователей портативных компьютеров настраивается в роуминг клиентов. Когда такие компьютеры подключены к внутренней сети по модему, им присваивается наилучший родительский сервер исходя из скорости и географической близости. Symantec AntiVirus Corporate Edition проверяет наличие обновлений и может получать небольшие файлы настройки для изменения значений параметров.
- Рабочие станции, не попадающие ни в одну специальную категорию, используют общий родительский сервер. К каждому родительскому серверу подключено не более 5 000 клиентов. Такие клиенты устанавливают сеансы связи с родительским сервером каждые 200 минут.
- Symantec AntiVirus Corporate Edition передает зараженные файлы, которые не удалось вылечить, серверу Центрального изолятора. Подозрительные файлы передаются в Symantec Security Response через Digital Immune System для анализа. Система Digital Immune System (DIS) анализирует полученную информацию и либо возвращает новое описание вируса в шлюз DIS, либо передает файл в Symantec Security Response для дальнейшего анализа.
- Клиенты настраиваются таким образом, что если пользователь отключит постоянную защиту файловой системы, она будет автоматически включена через тридцать минут.
- Администратор планирует осмотр серверной группы для проверки всех серверов Symantec AntiVirus Corporate Edition в нерабочее время. Осмотр запланирован на время, не совпадающее с временем

выполняющегося каждую ночь резервного копирования, с тем, чтобы эти задачи не пересекались друг с другом.

- Администратор также составляет план еженедельного осмотра клиентов. В окне Параметры клиента (только для администратора) Symantec AntiVirus Corporate Edition был выбран параметр приостановки планового осмотра, если клиент работает от батарей. Поэтому, если переносной компьютер питается от батарей, то плановый осмотр будет отложен до того момента, когда будет восстановлено обычное питание.
- Пользователям из группы клиентов, созданной для отдела продаж, разрешается приостанавливать плановый осмотр. Если плановый осмотр начнется во время выполнения важной задачи, например, представления товара, пользователь может нажать кнопку «Отложить», чтобы отложить осмотр на три часа. Осмотр можно отложить таким образом не более двух раз.
- На компьютерах с операционной системой Windows настраиваются ресурсы процессора, занимаемые при ручном или плановом осмотре. Это позволяет загружать процессор в промежутки времени, когда он простаивает, минимизируя тем самым влияние на обычную работу пользователя.

Обновление описаний вирусов в очень большой организации

Очень большие организации обновляют описания вирусов следующим образом:

- Один сервер Windows 2000 в центральном офисе назначается главным первичным сервером. Этот сервер получает обновления описаний от компании Symantec с помощью функции LiveUpdate.
- Остальные первичные серверы получают обновления от главного в заданное время и с заданной периодичностью. Затем первичные серверы передают файлы обновления на родительские серверы. Родительские серверы обновляют несколько клиентов одновременно, по одному клиенту в каждом сегменте сети, чтобы сократить сетевой трафик.
- Большинство мобильных пользователей получают описания вирусов от присвоенного им родительского сервера роуминга. Файлы описания вирусов имеют небольшой размер и не занимают много времени при передаче по модемному соединению. Кроме того, мобильные пользователи могут воспользоваться функцией Continuous LiveUpdate для получения обновлений непосредственно с сайта Symantec по сети

Internet. Администраторы задали максимальный срок использования устаревших файлов описания вирусов на компьютере Symantec AntiVirus Corporate Edition, после чего обновление запускается принудительно. После того как клиент Symantec AntiVirus Corporate Edition определит, что максимальный возраст файлов описания вирусов превышен, при наличии соединения с Интернет автоматически запускается автономный сеанс LiveUpdate.

- Сценарий регистрации мобильных пользователей с подключением по модему автоматически запускает LiveUpdate для обновления описаний вирусов после регистрации на сервере RAS/VPN.

Глава 3

Средство Reset ACL

Эта глава содержит следующие разделы:

Общие сведения о средстве Reset ACL

Средство Reset ACL (Resetacl.exe) позволяет ограничить доступ к разделам реестра Windows XP/2000/NT 4.0, относящимся к Symantec AntiVirus Corporate Edition.

По умолчанию всем пользователям разрешено изменять данные реестра, связанные с любым приложением, включая Symantec AntiVirus Corporate Edition. Средство Reset ACL аннулирует полные права доступа всех пользователей к следующим разделам и подразделам Symantec AntiVirus Corporate Edition в реестре:

HKLM\SOFTWARE\Intel\LANDesk\VirusProtect6\CurrentVersion

Ограничение доступа к реестру с помощью Reset ACL

Средство Reset ACL применяется для ограничения доступа к реестру.

Для ограничения доступа к реестру с помощью Reset ACL

1. Установите Resetacl.exe, расположенный в папке Tools компакт-диска Symantec AntiVirus Corporate Edition, на незащищенные компьютеры.
2. Запустите Resetacl.exe на всех таких компьютерах.

После запуска Resetacl.exe изменять значения реестра смогут только пользователи с правами администратора.

Хотя средство Reset ACL и повышает уровень безопасности при работе Symantec AntiVirus Corporate Edition, следует принять во внимание и некоторые побочные эффекты.

Помимо запрета на работу с реестром, пользователи без прав администратора не смогут выполнять следующие действия:

- Запускать или останавливать службу Symantec AntiVirus Corporate Edition;
- Запускать LiveUpdate;
- Задавать расписание сеансов LiveUpdate;
- Настраивать Symantec AntiVirus Corporate Edition.

  Например, они не смогут включить постоянную защиту или настроить параметры проверки электронной почты.

Соответствующие параметры будут показаны в интерфейсе Symantec AntiVirus Corporate Edition серым цветом.

Кроме того, пользователи смогут изменять параметры осмотра, но эти изменения не будут сохраняться в реестре и не вступят в силу. Пользователи также смогут сохранять параметры ручного осмотра для использования по умолчанию, но эти параметры также не будут записаны в реестр.

Глава 4

Средство Importer

Эта глава содержит следующие разделы:

Общие сведения о средстве Importer

Средство Importer (Importer.exe) позволяет идентифицировать компьютеры для консоли Symantec System Center вне среды WINS. С его помощью Symantec AntiVirus Corporate Edition может обнаруживать компьютеры в сети даже в том случае, если службы WINS/DNS недоступны. Это средство нужно вызывать из командной строки.

Кроме импорта пар имен и IP-адресов компьютеров, расположенных в средах, которые не поддерживают WINS, имеется возможность добавить любую другую пару имени компьютера и IP-адреса в текстовый файл с тем, чтобы этот компьютер обнаруживался в дальнейшем. Например, таким способом можно добавить имя и адрес компьютера, который не был обнаружен по неустановленной причине.

Примечание: В большинстве случаев средство Importer не требуется. Обычно Symantec System Center обнаруживает серверы Symantec AntiVirus Corporate Edition в сети с помощью функции «Найти компьютер» и стандартных процедур кэширования и обнаружения адресов.

Как работает средство Importer

Средство Importer запускается на любом компьютере, на котором установлен Symantec System Center. Это средство можно использовать для импорта пар имен компьютеров и IP-адресов из текстового файла в записи реестра кэша адресов, используемого Symantec System Center.

После импорта пар имен компьютеров и адресов создаются записи в следующем разделе реестра:

HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\AddressCache

После импорта файла с данными необходимо запустить локальное обнаружение или интенсивное обнаружение. Функция обнаружения опрашивает компьютеры по адресам. Компьютеры, на которых работает сервер Symantec AntiVirus Corporate Edition, добавляются службой обнаружения в память и для них заполняются записи, созданные в реестре. После этого служба обнаружения сможет находить эти компьютеры при каждом запуске службы.

Где находится средство Importer

Средство Importer состоит из одного файла Importer.exe, который расположен на компакт-диске Symantec AntiVirus Corporate Edition в папке Tools.

Перед запуском средство Importer.exe можно скопировать в любую папку компьютера, на котором установлен Symantec System Center.

Импорт адресов с помощью средства Importer

Для того чтобы импортировать адреса в кэш адресов, необходимо войти в систему с правами администратора. Это позволит получить доступ к разделу HKEY_LOCAL_MACHINE для записи.

Импорт адресов с помощью средства Importer

Для импорта адресов с помощью средства Importer необходимо выполнить следующие действия:

- Создать файл данных, содержащий пары имен компьютеров и IP-адресов.
- Запустить средство Importer.

  Примечание: Средство Importer следует запускать из командной строки.

- Запустить службу обнаружения.

Создание файла данных

1. Создайте новый файл с помощью текстового редактора, например, Блокнота.
2. Введите данные в следующем формате:

   <имя сервера><запятая><IP-адрес><перевод строки>

   Избегайте указывать неверные IP-адреса серверов. Текстовый файл для средства Importer не проверяется на предмет наличия серверов с одинаковыми IP-адресами.
3. Сохраните файл.

   Например, файл данных с именем Computers.txt может выглядеть следующим образом.

Computer 1, 155.64.3.121
Computer 2, 155.64.3.122
Computer 3, 155.64.3.123
Computer 4, 155.64.3.124
Computer 5, 155.64.3.125
Computer 6, 155.64.3.126

Примечание: Для того чтобы «закомментировать» адрес, введите слева от него точку с запятой или двоеточие. Например, если известно, что определенный сегмент сети отключен, можно закомментировать относящиеся к этому сегменту или подсети адреса.

Запуск средства Importer

1. В командной строке введите следующую команду:
   <полный путь> importer <имя файла>
   где <полный путь> — это полное имя каталога средства Importer, а <имя файла> — полное имя импортируемого файла, например, C:\Computers\Computers.txt
2. Нажмите клавишу **Enter**.

Удаление записей из кэша адресов

Данные, импортированные из файла, не заменяют собой данные, уже находящиеся в кэше адресов. Если некоторые данные необходимо удалить (например, если они содержат неправильный адрес компьютера), то перед вызовом программы Importer очистите кэш адресов.

Примечание: Не нажимайте кнопку «Очистить кэш» после импорта данных из файла. Эта операция удалит из кэша все данные, включая только что импортированные из файла.

Удаление записей из кэша адресов

1. В меню «Сервис» консоли Symantec System Center выберите команду **Служба обнаружения**.
2. В разделе «Информация кэша» нажмите «**Очистить кэш**».

После импорта данных вызовите функцию обнаружения, чтобы данные стали доступны для последующих сеансов.

Дополнительные возможности

В команде предусмотрены четыре параметра:

- Путь к файлу импорта
- Первый разделитель
- Второй разделитель
- Порядок (1 = имя компьютера/IP-адрес, 2 = IP-адрес/имя компьютера; по умолчанию — 1)

Примечание: В качестве второго разделителя допустим только один символ. Например, символ амперсанда недопустим, поскольку пользователю придется ввести следующую строку: «&»

Например, файл импорта Machines.txt в каталоге C:\MACHINES может выглядеть следующим образом:

155.64.3.121/Server 1

155.64.3.122/Server 2

155.64.3.123/Server 3

В приведенном выше примере применяется порядок IP-адрес/имя компьютера (2). Первый параметр — косая черта (/), а второй — перевод строки. Такому формату соответствует следующий синтаксис вызова команды:

importer C:\MACHINES\Machines.txt / LF 2

После импорта пар имен компьютеров и адресов создаются записи в следующем разделе реестра:

HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\AddressCache

После импорта файла с данными необходимо запустить локальное или интенсивное обнаружение. В процессе обнаружения у компьютеров будут запрошены их IP-адреса. Компьютеры, на которых работает Symantec AntiVirus Corporate Edition, добавляются службой обнаружения в память, и для них заполняются записи, созданные в реестре. После этого служба обнаружения сможет находить эти компьютеры при каждом запуске службы.

Получение справки по работе со средством Importer

Средство Importer содержит справочную информацию о переключателях и синтаксисе.

Получение справки по работе со средством Importer

1. В командной строке введите следующую команду:
   Importer
2. Нажмите клавишу **Enter.**

Средство Importer покажет следующую справочную информацию:

```
Простой формат: IMPORTER <имя файла>

<имя файла> : полный путь к файлу импорта

Формат файла: <имя сервера><запятая><IP-адрес><перевод строки>

Пример файла: Server 1,155.64.3.121

Server 2,155.64.3.122

Server 3,155.64.3.123

нажмите "a" для получения дополнительной информации

После нажатия клавиши "a" будет показана следующая информация:

Дополнительные возможности: IMPORTER <имя файла> <разделитель 1>
<разделитель 2> <порядок>

<имя файла> : полный путь к файлу импорта

<разделитель 1> : разделитель между первым и вторым элементом пары

<разделитель 2> : разделитель между парами

ПРИМЕЧАНИЕ: для указания перевода строки применяется сочетание LF

для указания пробела применяется сочетание SP

для указания запятой применяется ,

<порядок> : порядок элементов в паре "имя компьютера/ip-адрес"

1 = имя компьютера/ip-адрес

2 = ip-адрес/имя компьютера

ПРИМЕР -

Содержимое файла: 155.64.3.121/Server 1

155.64.3.122/Server 2

155.64.3.123/Server 3

Команда: IMPORTER C:\MyFolder\MyFile.txt / LF 2
```

Известные проблемы

Средство Importer использует раздел реестра HKLM\SOFTWARE\Intel\LANDesk\VirusProtect6\CurrentVersion\AddressCache, принадлежащий Symantec System Center. Если этот раздел отсутствует, то будет показано сообщение об ошибке.

Средство Importer изменяет параметр AddressCache в разделе HKLM, поэтому пользователю необходимы права администратора.

Средство Importer применяется функцией обнаружения компьютеров Symantec System Center. Средство Importer пытается определить, установлен ли на локальном компьютере Symantec System Center. Если он не установлен, то появляется сообщение об ошибке.

Непосредственно после импорта пары «имя компьютера/IP-адрес» в реестре будут неполны. В параметрах dword Address_0 и Protocol будет показано только имя компьютера. Для завершения процесса необходимо запустить обнаружение (кнопка «Начать обнаружение» в окне «Свойства службы обнаружения»).

Не нажимайте в окне «Свойства службы обнаружения» кнопку «Очистить кэш». Эта операция удалит из кэша все данные, включая импортированные из файла.

Средство Importer не предназначено для поиска компьютеров в процессе установки.

Примечание: При установке клиента или сервера Symantec AntiVirus Corporate Edition на удаленных компьютерах в окне «Выбор компьютера» появится параметр «Импорт». Не путайте этот параметр с параметром «Импорт» на экранах «Установка клиента NT» и «Установка сервера AV».

Средство Importer разработано таким образом, что оно не удаляет существующие IP-адреса из кэша адресов. Иногда в кэш адресов ошибочно заносятся неверные IP-адреса. Средство Importer не сможет их исправить.

Глава 5

Службы Windows XP/2000/NT

Эта глава содержит следующие разделы:

Службы Symantec AntiVirus Corporate Edition

В Табл. 5-1 приведены имена и описания служб сервера Symantec AntiVirus Corporate Edition. Имена представлены в том формате, в котором они показаны на панели управления службами Windows XP/2000/NT.

Табл. 5-1 Службы сервера Symantec AntiVirus Corporate Edition

Имя службы	Имя файла	Описание
Сервер Symantec AntiVirus	Rtvscan.exe	Основная служба Symantec AntiVirus Corporate Edition. Большинство задач сервера Symantec AntiVirus Corporate Edition выполняется этой службой.
Defwatch	Defwatch.exe	Служба, отслеживающая появление новых описаний. При получении обновленных описаний вирусов запускает осмотр файлов в Изоляторе.
Intel PDS	Pds.exe	Служба Ping Discovery Service. Обеспечивает возможность обнаружения Symantec AntiVirus Corporate Edition на компьютере. Приложения регистрируются этой службой как с помощью идентификаторов APP ID, так и с помощью ответных (pong) пакетов, возвращаемых в ответ на запросы (ping).

В Табл. 5-2 приведены имена и описания служб клиента Symantec AntiVirus Corporate Edition. Имена представлены в том формате, в котором они показаны на панели управления службами Windows XP/2000/NT.

Табл. 5-2 Службы клиента Symantec AntiVirus Corporate Edition

Имя службы	Имя файла	Описание
Клиент Symantec AntiVirus	Rtvscan.exe	Основная служба Symantec AntiVirus Corporate Edition. Большинство задач клиента Symantec AntiVirus Corporate Edition выполняется этой службой.
Defwatch	Defwatch.exe	Служба, отслеживающая появление новых описаний. При получении обновленных описаний вирусов запускает осмотр файлов в Изоляторе.

Службы Symantec System Center

В Табл. 5-3 приведены имена и описания служб Symantec System Center. Имена представлены в том формате, в котором они показаны на панели управления службами Windows XP/2000/NT.

Табл. 5-3 Службы Symantec System Center

Имя службы	Имя файла	Описание
Служба обнаружения Symantec System Center	Nsctop.exe	Служба обнаружения позволяет находить в сети серверы Symantec AntiVirus Corporate Edition. Кроме того, служба обнаружения передает объекты консоли.

В Табл. 5-4 приведены имена и описания служб Alert Management System[2]. Имена представлены в том формате, в котором они показаны на панели управления службами Windows XP/2000/NT.

Табл. 5-4 Службы Alert Management System[2]

Имя службы	Имя файла	Описание
Intel Alert Handler	Hndlrsvc.exe	Служба обработки оповещений AMS[2]. Обеспечивает выполнение оповещающих действий, например, вывод сообщений на экран, отправку на пейджер, по электронной почте и т. д.
Intel Alert Originator	Iao.exe	Служба получения оповещений AMS[2]. Обеспечивает получение оповещений компьютером. Оповещения можно получать как с локального компьютера (если это первичный сервер), так и с удаленных компьютеров (если это автономные клиенты, использующие центральный сервер AMS[2]).
Intel File Transfer	Xfr.exe	Служба передачи файлов. Обеспечивает функции передачи файлов для системы AMS[2].
Intel PDS	Pds.exe	Служба Ping Discovery Service. Обеспечивает возможность обнаружения Symantec AntiVirus Corporate Edition на компьютере. Приложения регистрируются этой службой как с помощью идентификаторов APP ID, так и с помощью ответных (pong) пакетов, возвращаемых в ответ на запросы (ping).

Глава 6

Записи журнала событий Windows XP/2000/NT

События Symantec AntiVirus Corporate Edition

В Табл. 6-1 перечислены события, заносимые в журнал Windows XP/2000/NT программой Symantec AntiVirus Corporate Edition.

Табл. 6-1 События, заносимые в журнал событий Windows

Событие	Номер события	Описание
Event_Scan_Stop	2	Возникает при завершении осмотра.
Event_Scan_Start	3	Возникает при начале осмотра.
Event_Pattern_Update	4	Возникает при отправке файла .vdb от родительского сервера вторичному.
Event_Infection	5	Возникает в случае, если при осмотре обнаружен вирус.
Event_File_Not_Open	6	Возникает в случае, если при осмотре не удалось получить доступ к файлу или каталогу.
Event_Load_Pattern	7	Возникает при загрузке программой Symantec AntiVirus Corporate Edition нового файла .vdb.

Табл. 6-1 События, заносимые в журнал событий Windows

Событие	Номер события	Описание
Event_Trap	11	Возникает при осмотре почтовых вложений, если включена постоянная защита электронной почты.
Event_Config_Change	12	Возникает внесении в конфигурацию сервера изменений, введенных с консоли, за исключением изменения разделов реестра PRODUCTCONTROL и DOMAINDATA..
Event_Shutdown	13	Возникает при выгрузке службы Symantec AntiVirus Corporate Edition.
Event_Startup	14	Возникает при загрузке службы Symantec AntiVirus Corporate Edition.
Event_Pattern_Download	16	Возникает при загрузке новых описаний во время планового обновления описаний.
Event_Too_Many_Viruses	17	Возникает в случае, если Symantec AntiVirus Corporate Edition удалил или изолировал более 5 зараженных файлов за последнюю минуту. Интервал времени, а также число изолированных или удаленных файлов можно настроить с помощью реестра. По умолчанию эти значения составляют 5 файлов и 60 секунд.
Event_Fwd_To_Qserver	18	Возникает при отправке изолированных файлов на сервер изолятора.

Табл. 6-1 События, заносимые в журнал событий Windows

Событие	Номер события	Описание
Event_Backup_Restore_Error	20	Возникает в случае, если Symantec AntiVirus Corporate Edition не смог сохранить или восстановить файл из изолятора.
Event_Scan_Abort	21	Возникает в случае, если осмотр был остановлен до полного завершения.
Event_Rts_Load_Error	22	Возникает, если не удалось загрузить AutoProtect.
Event_Rts_Load	23	Возникает при успешной загрузке AutoProtect.
Event_Rts_Unload	24	Возникает при успешной выгрузке AutoProtect.
Event_Remove_Client	25	Возникает в случае, когда родительский сервер удаляет клиентский компьютер из списка клиентов. По умолчанию это означает, что клиентский компьютер не регистрировался на родительском сервере в течение более 30 дней.
Event_Scan_Delayed	26	Возникает в случае, если плановый осмотр был задержан (отложен).
Event_Scan_Restart	27	Возникает при перезапуске отложенного осмотра.

Алфавитный указатель

Обслуживание и техническая поддержка

Компания Symantec стремится обеспечивать высокое качество обслуживания клиентов во всем мире. Она предоставляет помощь профессионалов в любой точке мира для решения вопросов, связанных с применением программного обеспечения и услуг.

Порядок обслуживания клиентов и технической поддержки в разных странах различен.

Если у вас возникнут вопросы относительно описанных ниже услуг, обратитесь к разделу «Центры обслуживания клиентов и технической поддержки».

Регистрация и лицензии

Если для работы с продуктом необходима регистрация или код лицензии, рекомендуем вам обратиться на Web-сайт регистрации и лицензирования фирмы Symantec, расположенный по адресу www.symantec.com/certificate. Кроме того, можно обратиться по адресу http://www.symantec.com/techsupp/ent/enterprise.html, выбрать программный продукт, который необходимо зарегистрировать, и воспользоваться соответствующей ссылкой для лицензирования и регистрации на домашней странице этого продукта.

Если вы приобрели подписку на техническую поддержку, то для решения технических вопросов можно обратиться в компанию Symantec по телефону или через Интернет. При первом обращении в службу технической поддержки будьте готовы назвать номер вашего лицензионного сертификата или контактный идентификатор, полученный при регистрации продукта, чтобы сотрудники службы поддержки могли

проверить ваше право на получение соответствующей услуги. Если вы не приобрели подписку на техническую поддержку, то для получения подробных сведений о предоставляемых услугах технической поддержки обратитесь в отдел обслуживания клиентов фирмы Symantec или по месту приобретения продукта.

Обновление средств защиты

Самые последние сведения о вирусах и потенциальных угрозах можно получить на Web-сайте Symantec Security Response (ранее называвшемся Центром антивирусных исследований – Antivirus Research Center) по адресу:

http://securityresponse.symantec.com

На этом сайте представлены обширные сведения по вопросам обеспечения безопасности и о вирусных угрозах, а также новейшие файлы описаний вирусов. Описания вирусов также можно загрузить с помощью функции LiveUpdate, входящей в состав программных продуктов.

Продление подписки на получение антивирусных обновлений

Приобретение вместе с программным продуктом пакета услуг по его обслуживанию позволяет загружать бесплатные обновления описаний вирусов на протяжении срока действия договора об обслуживании. Если срок действия договора об обслуживании закончился, обратитесь по месту приобретения продукта или в отдел обслуживания клиентов компании Symantec за информацией об условиях продления договора об обслуживании.

Web-сайты компании Symantec

Домашняя страница Symantec на различных языках

На английском языке:	http://www.symantec.com
На русском языке:	http://www.symantec.ru
На французском языке:	http://www.symantec.fr
На немецком языке:	http://www.symantec.de
На итальянском языке:	http://www.symantec.it
На голландском языке:	http:// www.symantec.nl

Symantec Security Response

http://securityresponse.symantec.com

Страница Symantec Enterprise Service and Support

http://www.symantec.com/techsupp/bizsolutions/

Бюллетени новостей для отдельных продуктов

США и Азиатско-Тихоокеанский регион, на английском языке:

http://www.symantec.com/techsupp/bulletin/index.html

Европа, Ближний Восток и Африка, на английском языке:

http://www.symantec.com/region/reg_eu/techsupp/bulletin/index.html

На французском языке:

http://www.symantec.com/region/fr/techsupp/bulletin/index.html.

На немецком языке:

http://www.symantec.com/region/de/techsupp/bulletin/index.html

На голландском языке:

http://www.symantec.com/region/nl/techsupp/bulletin/index.html

На итальянском языке:

http://www.symantec.com/region/it/techsupp/bulletin/index.html

Техническая поддержка

Являясь составной частью центра Symantec Security Response, наша группа глобальной технической поддержки обеспечивает работу центров поддержки по всему миру. Нашей основной деятельностью являются ответы на вопросы о функциях и программных продуктах, их установке и настройке, а также пополнение базы знаний, доступной через Интернет. Мы работаем в тесном сотрудничестве с другими подразделениями компании Symantec, что позволяет отвечать на ваши вопросы в кратчайшие сроки. Например, мы сотрудничаем с отделом разработки продуктов и с антивирусными исследовательскими центрами для обеспечения работы служб оповещения и обновления описаний вирусов в случае распространения новых вирусов и для рассылки оповещений. Мы предлагаем следующие услуги:

- Различные варианты поддержки, позволяющие выбрать набор необходимых услуг для организации любого размера;
- Предоставление поддержки по телефону и через Интернет, что позволяет найти решение в кратчайшие сроки и получить самую свежую информацию;
- Обновления программных продуктов, позволяющие автоматически обновлять средства защиты;
- Обновления сигнатур и описаний вирусов, обеспечивающие высокий уровень безопасности;
- Глобальная поддержка с участием специалистов центра Symantec Security Response, доступная ежедневно и круглосуточно по всему миру на нескольких языках;
- Дополнительные функции, такие как служба оповещения Symantec и возможность назначения менеджера по техническим вопросам, расширяющие возможности для получения эффективной и профессиональной поддержки.

Сведения о предлагаемых в настоящее время программах поддержки можно получить на нашем Web-сайте.

Что необходимо для обращения в службу поддержки

Пользователи, заключившие договор о технической поддержке, могут обращаться в службу технической поддержки по телефону или через Интернет по следующему адресу или по адресу одного из указанных ниже Web-сайтов региональной службы поддержки.

www.symantec.com/techsupp/ent/enterprise.html

При обращении в службу поддержки вам потребуется сообщить следующую информацию:

- Номер версии программного продукта
- Сведения об аппаратном обеспечении
- Объем оперативной памяти, емкость диска, сведения о сетевом адаптере
- Сведения об операционной системе
- Номер версии и пакета обновления
- Топология сети
- Сведения о маршрутизаторе, шлюзе и IP-адресах
- Описание возникших неполадок
- Сообщения об ошибках, файлы журналов
- Действия по устранению неполадок, выполненные перед обращением в компанию Symantec
- Сведения об изменениях, недавно внесенных в конфигурацию программного обеспечения или сети

Обслуживание клиентов

В Центре обслуживания клиентов компании Symantec можно получить сведения по вопросам, не связанным с технической поддержкой, например:

- Общие сведения о продукте (например, основные функции, поддерживаемые языки, торговые представительства в вашем регионе и т.д.)
- Основные методы устранения неполадок, например, как узнать версию продукта
- Последние данные об обновлениях программного продукта

- Инструкции по обновлению и модернизации программного продукта
- Инструкции по регистрации программного продукта или лицензии
- Сведения о программах лицензирования компании Symantec
- Информация о контрактах на льготное обновление и обслуживание
- Замена компакт-дисков и руководств
- Обновление регистрационных данных в связи с изменением адреса или имени владельца программного продукта
- Описание различных вариантов технической поддержки, предлагаемых компанией Symantec

Подробные сведения об обслуживании клиентов можно получить на Web-сайте обслуживания и поддержки компании Symantec, а также в центре обслуживания клиентов компании Symantec. Номера телефонов и адреса Web-сайтов центра обслуживания клиентов, расположенного в вашем регионе, можно найти в разделе «Центры обслуживания клиентов и технической поддержки», приведенном в конце главы.

Центры обслуживания клиентов и технической поддержки

Европа, Ближний Восток и Африка

Web-сайты обслуживания и технической поддержки компании Symantec

На английском языке:	www.symantec.com/eusupport/
На французском языке:	www.symantec.fr/frsupport
На немецком языке:	www.symantec.de/desupport/
На итальянском языке:	www.symantec.it/itsupport/
На голландском языке:	www.symantec.nl/nlsupport/
FTP-сайт компании Symantec: (Загрузка сведений по техническим вопросам и последних пакетов обновлений)	ftp.symantec.com

Посетите Web-сайты обслуживания и технической поддержки компании Symantec, на которых можно найти технические и общие сведения о различных программных продуктах.

Symantec Security Response

http://securityresponse.symantec.com

Бюллетени новостей для отдельных продуктов

США, на английском языке:

http://www.symantec.com/techsupp/bulletin/index.html

Европа, Ближний Восток и Африка, на английском языке:

http://www.symantec.com/region/reg_eu/techsupp/bulletin/index.html

На французском языке:

http://www.symantec.com/region/fr/techsupp/bulletin/index.html

На немецком языке:

http://www.symantec.com/region/de/techsupp/bulletin/index.html

На голландском языке:

http://www.symantec.com/region/nl/techsupp/bulletin/index.html

На итальянском языке:

http://www.symantec.com/region/it/techsupp/bulletin/index.html

Отдел обслуживания клиентов компании Symantec

Для получения информации, не касающейся технических вопросов, и рекомендаций по выполнению ряда задач можно обратиться по указанным ниже телефонам на одном из следующих языков: английском, немецком, французском или итальянском:

Австрия	+ (43) 1 50 137 5030
Бельгия	+ (32) 2 2750173
Великобритания	+ (44) 20 7744 0367
Германия	+ (49) 69 6641 0315
Дания	+ (45) 35 44 57 04
Ирландия	+ (353) 1 811 8093
Испания	+ (34) 91 7456467
Италия	+ (39) 02 48270040
Люксембург	+ (352) 29 84 79 50 30
Нидерланды	+ (31) 20 5040698

Норвегия	+ (47) 23 05 33 05
Финляндия	+ (358) 9 22 906003
Франция	+ (33) 1 70 20 00 00
Швеция	+ (46) 8 579 29007
Швейцария	+ (41) 2 23110001
ЮАР	+ (27) 11 797 6639
Прочие страны (только на английском языке)	+ (353) 1 811 8093

Почтовый адрес отдела обслуживания клиентов компании Symantec

Symantec Ltd
Customer Service Centre
Europe, Middle East and Africa (EMEA)
PO Box 5689
Dublin 15
Ireland

Сведения для клиентов из Азиатско-Тихоокеанского региона

Компания Symantec обеспечивает техническую поддержку и обслуживание клиентов по всему миру. В различных странах обслуживание клиентов организовано по-разному. В частности, в некоторых регионах нет представительства компании Symantec, и указанные услуги предоставляются международными партнерами Symantec. Для получения общей информации обратитесь в региональный отдел обслуживания и поддержки компании Symantec.

Отделы обслуживания клиентов и технической поддержки

Австралия

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Australia

Основной номер телефона	+61 2 8879 1000	
Факс	+61 2 8879 1001	
Web-сайт	http://service.symantec.com	
Техническая поддержка по плану Gold	1800 805 834	gold.au@symantec.com
Информация о контрактах технической поддержки	1800 808 089	contractsadmin@symantec.com

Гонконг

Symantec Hong Kong
Central Plaza
Suite #3006
30th Floor, 18 Harbour Road
Wanchai
Hong Kong

Основной номер телефона	+852 2528 6206
Техническая поддержка	+852 2528 6206
Факс	+852 2526 2646
Web-сайт	http://www.symantec.com.hk

Индия

Symantec India
Suite #801
Senteck Centrako
MMTC Building
Bandra Kurla Complex
Bandra (East)
Mumbai 400051, India

Основной номер телефона	+91 22 652 0658
Факс	+91 22 652 0671
Web-сайт	http://www.symantec.com/india
Техническая поддержка:	+91 22 657 0669

Китай

Symantec China
Unit 1-4, Level 11,
Tower E3, The Towers, Oriental Plaza
No.1 East Chang An Ave.,
Dong Cheng District
Beijing 100738
China P.R.C.

Основной номер телефона	+86 10 8518 3338
Техническая поддержка	+86 10 8518 6923
Факс	+86 10 8518 6928
Web-сайт	http://www.symantec.com.cn

Корея

Symantec Korea
15,16th Floor
Dukmyung B/D
170-9 Samsung-Dong
KangNam-Gu
Seoul 135-741
South Korea

Основной номер телефона	+822 3420 8600
Факс	+822 3452 1610
Техническая поддержка	+822 3420 8650
Web-сайт	http://www.symantec.co.kr

Малайзия

Symantec Corporation (Malaysia) Sdn Bhd
31-3A Jalan SS23/15
Taman S.E.A.
47400 Petaling Jaya
Selangor Darul Ehsan
Malaysia

Основной номер телефона	+603 7805 4910
Факс	+603 7804 9280
Электронный адрес для юридических лиц	gold.apac@symantec.com
Номер телефона для бесплатных звонков	1800 805 104
Web-сайт	http://www.symantec.com.my

Новая Зеландия

Symantec New Zealand
Level 5, University of Otago Building
385 Queen Street
Auckland Central 1001
New Zealand

Основной номер телефона	+64 9 375 4100	
Факс	+64 9 375 4101	
Web-сайт службы технической поддержки	http://service.symantec.co.nz	
Техническая поддержка по плану Gold	0800 174 045	gold.nz@symantec.com
Информация о контрактах технической поддержки	0800 445 450	contractsadmin@symantec.com

Сингапур

Symantec Singapore
3 Phillip Street
#17-00 & #19-00 Commerce Point
Singapore 048693

Основной номер телефона	+65 6239 2000
Факс	+65 6239 2001
Техническая поддержка	+65 6239 2099
Web-сайт	http://www.symantec.com.sg

Тайвань

Symantec Taiwan
2F-7, No.188 Sec.5
Nanjing E. Rd.,
105 Taipei
Taiwan

Основной номер телефона	+886 2 8761 5800
Техническая поддержка для организаций	+886 2 8761 5800
Факс	+886 2 2742 2838
Web-сайт	http://www.symantec.com.tw

Мы сделали все возможное, чтобы представленная здесь информация была полной и точной. Тем не менее, содержащаяся в настоящем документе информация может быть изменена безо всякого уведомления. Корпорация Symantec оставляет за собой право на внесение таких изменений без предварительного уведомления.